UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/328,726	10/26/1998	THOMAS COLLINS	2026-25(PT-TA 410(Contl)	7212

7590 06/03/2004

HEWLETT-PACKARD COMPANY
Attn: Bill Streeter
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SEAL, JAMES	
ART UNIT	PAPER NUMBER
2135	32

DATE MAILED: 06/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action	**Application No.** *09/328,726*	**Applicant(s)** COLLINS ET AL.
	Examiner James Seal	**Art Unit** 2135

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 28 April 2004 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE. Therefore, further action by the applicant is required to avoid abandonment of this application. A proper reply to a final rejection under 37 CFR 1.113 may only be either: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114.

PERIOD FOR REPLY [check either a) or b)]

a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.

b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection. ONLY CHECK THIS BOX WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

1.□ A Notice of Appeal was filed on _____. Appellant's Brief must be filed within the period set forth in 37 CFR 1.192(a), or any extension thereof (37 CFR 1.191(d)), to avoid dismissal of the appeal.

2.☒ The proposed amendment(s) will not be entered because:

(a) ☒ they raise new issues that would require further consideration and/or search (see NOTE below);

(b) □ they raise the issue of new matter (see Note below);

(c) □ they are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d) □ they present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: *See Continuation Sheet.*

3.□ Applicant's reply has overcome the following rejection(s): _____.

4.□ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

Ka 5.☑ The a)□ affidavit, b)□ exhibit, or c)☑ request for reconsideration has been considered but does NOT place the application in condition for allowance because: See attachment

Ka 6.□ The affidavit or exhibit will NOT be considered because it is not directed SOLELY to issues which were newly raised by the Examiner in the final rejection.

7.☑ For purposes of Appeal, the proposed amendment(s) a)☑ will not be entered or b)□ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: 17-66, 73-112

Claim(s) withdrawn from consideration: _____.

8.□ The drawing correction filed on _____ is a)□ approved or b)□ disapproved by the Examiner.

9.□ Note the attached Information Disclosure Statement(s)(PTO-1449) Paper No(s). _____.

10.□ Other: _____

Continuation Sheet (PTOL-303) Application No.
09/328,726

Continuation of 2. NOTE: Claims 113-122 would require new searching. Further, some of these claims involve digital signatures which the examiner has already questioned as to whether their was support for this material with regards to cancelled claims 1-16.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Advisory Action

Response to Arguments

1. Applicant's arguments filed 28 April 2004 have been fully considered but they are not persuasive.

2. With regards to the admissibility of the Nemo paper "RSA Moduli Should Have 3 Prime Factors" dated August 1996:

Examiner argues that Protein Foundation v. Brenner does not apply to the Nemo paper since it is not a traditionally printed magazine. Examiner notes that the argument of choosing a later date than published is based on the inherent latency of the U.S. Post Office. Thus, arguing the applicability of Protein Foundation v. Brenner to the Nemo paper is equivalent to arguing the applicability of the attributes of the U.S. Post Office to an electronic publication. However, the Nemo paper was published electronically which assured a virtually instantaneous distribution, effectively bypassing the U.S. Post Office.

Additionally, MPEP 2128 (Section Titled: "Electronic Publications As Prior Art") states:

"Prior art disclosures on the Internet or on an on-line database are considered to be publicly available as of the date the item was publicly posted."

According to the copyleft date, the posting date is August 1996.

Applicant's assertion that the Nemo publication has not been published in such a manner that anyone who chose might avail themselves of the information it contains, is equivalent to stating that the Nemo copyleft date statement is in error.

Note that MPEP 2121.01 states that the test of applicability is whether an enabling disclosure is provided, which is the case regarding the Nemo paper. Furthermore, Examiner is required to presume that a reference's attributes are accurate and enabled in it's entirety, unless evidence to the contrary is presented. However, existence of Applicant's specification provides evidence that the Nemo reference is accurate. As a result, Examiner has no reason to assume that the Nemo reference is accurate in all aspects, except for the copyleft date. Thus, unless Applicant can provide evidence that the Nemo article's copyleft date is in error or otherwise materially misstated, Examiner must admit the August 1996 date.

Examiner reminds Applicant that Applicant has a duty of disclosure and full candor (37 CFR 1.56 and MPEP 2000). Examiner notes that the Nemo paper in question, was provided under Applicant's IDS. However, Applicant's IDS is silent as to the source of the Nemo paper, be it from a magazine, from a web site, or otherwise. 37 CFR 1.98 states:

"(5) Each publication listed in an information disclosure statement must be identified by publisher, author (if any), title, relevant pages of the publication, date, and place of publication."

If Applicant is in this possession of information that would properly invalidate the August 1996 date for the Nemo paper, Examiner directs Applicant to provide this information forthwith.

Finally, Examiner notes that the Nemo paper discloses a mathematical and universal truth, specifically, RSA moduli should have three prime factors. MPEP 2124 states:

"In Some Circumstances a Factual Reference Need Not Antedate the Filing Date.

In certain circumstances, references cited to show a universal fact need not be available as prior art before applicant's filing date. In re Wilson, 311 F.2d 266, 135 USPQ 442 (CCPA 1962). Such facts include the characteristics and properties of a material or a scientific truism. Some specific examples in which later publications showing factual evidence can be cited include situations where the facts shown in the reference are evidence "that, as of an application 's filing date, undue experimentation would have been required..."

Since the Nemo paper discloses a mathematical and universal truth, even if Applicant were to swear behind the August 1996 date, the Nemo paper would still be admissible as prior art.

3. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. Applicant argues that Lidl teaches absolutely nothing with respect to a desire to improve speed or save computation resources. With regards to Lidl, the reference was used to lay the mathematical foundations of multiprime RSA and to indicate that a knowledge of this art was available to those of ordinary skill in the art as far back as 1984, twelve years before the applicants submitted their invention in 1996. With regards to Lidl teachings, it would appear that the applicants would agree with the examiner that multiprime RSA was not new or original to their invention as they state that speed and conservation of resources not the multiprime RSA as taught in Lidl is what they consider important (see statement at the top of the second page of applicant's response in the remarks sections).

Quisquater disclose methods for speeding up RSA using parallel processing, made possible by the CRT decomposition (see Figure 1, sentence above equation (1) and next to the last line in paragraph under equation (1)), the recognition that performing computations with smaller rather than faster (see paragraph under equation (1);"the quantities p, q, c_1, c_2, d_1, d_2 are now about 300 bits long" as opposed to the ordinary RSA system in which the quanties such as "d would be about 500 or 600 bits long" and would further imply that storage of such quantities would require less memory and thus conservation of resources) and the elimination of any divisions in the computation (sentence above figure 1), application of these methods would increase the computational speed by a factor of 4 to 8 (Column 1, second paragraph). Thus one of ordinary skill in the art at the time the invention were made, would have recognized that by splitting n into multiple primes, that is the number of prime factors of n, would greatly increase the speed of a multi prime RSA. In the case of a 3 prime RSA, that would mean we would be performing computations on 200 bit number rather than 600 bit numers and with 6 prime RSA 100 bits rather than 600 bit numbers. This would be in addition to the parallelism offered by the CRT would further make the speed of processing faster due to the simultaneous rather than sequential processing. Further Lidl teaches the extension of the CRT to r simultaneous congruences (see 515-516) thus making the art available for the r prime case.

The combination Lidl/Quisquater is silent on the selection of random and distinct prime factors. Rivest teaches both random selection of prime factors of n as well as distinctness of the primes(see Rivest 6, line 34; page 9, lines 2-3 and 26-27) in order to maximize security. If one considers making p and q, that is p = q, the same, and hunt for primes in the interval $N_1 \leq p \leq N_2$, then the number of products of the form $n = p^2$ in the interval is smaller than of the form n = pq, this would mean that a brute force attack over the interval would be more successive over those of the form $n = p^2$ than n = pq. This would imply that the former is less secure. Thus one of ordinary skill in the art at the time that the invention was made, would have been motivated to have combined the teaching of the Lidl/Quisquater system with the teaching of Rivest (random distinct primes) as it would provide greater security for the system. This is further amplified in examiner last action see pages 4 and 5.

3. With regards to claims 18-66 the applicant argues that the addition of Ding to the combination Lidl/quisquater/Rivest is attacking the references separately for a rejection which is based on a combination of references. The Ding supplies the details of a

recursive algorithm which those in the art would have needed in order to implement the Lidl/quisquater/Rivest combination.

4. In response to applicant's argument that the examiner has combined an excessive number of references, reliance on a large number of references in a rejection does not, without more, weigh against the obviousness of the claimed invention. See *In re Gorman*, 933 F.2d 982, 18 USPQ2d 1885 (Fed. Cir. 1991).

5. With regards to the RSA/Revest/Quisquater/Knuth rejection, applicant implies that the number of references is excessive, that is four. The examiner would disagree. With the amount of mathematical details and corresponding limitations, four references is probably concise. The reference by Knuth, The art of Computer Programming, Vol. 2, page 179 is a well known reference for computational methods and was used to expand on what the prior art RSA, Rivest, and Quisquater in particular how the algorithms are applied in these references, that is fill in the details. RSA and Rivest represent the RSA patent and the journal article of the same. While they are not identical they are authored by the same authors and thus are used to get a better understanding of their invention.

6. With regards to RSA/Quisquater/Rivest/Ding rejection, applicant implies that the number of references is excessive, that is four. Again the examiner disagrees for the same reason as cited above. The RSA and Rivest references, in particular, describe the same invention of the same inventors and though they are not identical they describe the same invention from different viewpoints.

7. With regards to the combinations involving the Nemo reference see above.

8. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

9. With regards to the obviousness of the combinations, the examiner notes that in all of cases that the motivation to combine, is connected with making the original invention suggest in the RSA patent and the Rivest paper faster and more efficient without compromising its security. As pointed out by Quisquater and the other art one is limiting to several techniques, either to decrease the number of time consuming operations such as divisions, make use of techniques that can be possessed in parallel rather than sequentially or to decrease the size of the numbers (i.e. the number of digits) used in the computation, without decreasing the overall security of the system. The CRT provides part of the answer, in that it makes for parallel operations or to decrease the size of the primes use in the computation. The RSA, paper, the Lidl paper and the Nemo papers suggest that in order to do this one must increasing the number of prime factors in n while maintaining its size. The motivation is increased speed without compromising the security. The details of the motivations are slightly different

depending on which art is applied (see previous Action), but the motivation in all cases is the same.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JWS

Jws
Examiner AU2135
29 May 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100